SZ9-99-002

- 19 -

Claims

1. An access control system with a plurality of locks and keys, at least part of said locks and keys having memory means, characterized by

- said memory means of a key being equipped to receive and store information concerning any access rights of said key and information designated for other keys and/or locks,

- said memory means of a lock being equipped to receive and store information
10   concerning any access rights for said lock and information designated for other keys and/or locks, and

- means for exchanging said information between locks and keys.

2. The access control system according to claim 1, wherein
15 - the information concerning access rights of a key includes one or more tokens and/or the information designated for other keys and/or locks includes one or more messages for said keys and/or locks.

3. The access control system according to any of the preceding claims, wherein
20 - the memory means in the key and/or the lock stores at least a partial view of the system and

- the exchanging means triggers an update of said view.

4. The access control system according to claims 3, wherein
25 - the update triggered by the exchanging means is performed off-line, particularly right after said exchanging means has completed its function.

5. The access control system according to any of the preceding claims, wherein

- the information designated for other keys and/or locks includes one or more
30   messages for said other keys and/or locks and is exchanged off-line between a key and a lock.

6. The access control system according to one or more of the preceding claims, wherein

- the means for exchanging information between a lock and a key are activated when said key is engaged with said lock.

5

7. A key for use in an access control system according to any one of the preceding claims, wherein

- the memory means includes a read/write section dedicated to the information designated for other keys and/or locks.

10

8. The key according to claim 7, characterized by

- a power source, preferably being rechargeable when said key is used with a lock.

15

9. A lock for use in an access control system according to any one of the claims 1 to 6, wherein

- the memory means includes a read/write section dedicated to the information designated for other keys and/or locks.

20

10. The lock according to claim 9, characterized by

- a power source, preferably being rechargeable when a key is used with said lock.

25

11. A method for propagating information in an electronic lock-and-key system, characterized in that

- an original message to be propagated to an n-th lock or key is inserted into a memory of a first lock or a first lock, respectively,
- on any use of said first key or said first lock, said original message is copied into a memory of a second lock or key, respectively, but remains in said first

30

lock's or first key's, respectively, memory,

- on any subsequent use of said first and/or second key and/or said first and/or second lock, said original message is copied into a memory of a next lock or

key, respectively, but remains in the memories of said previously used locks and/or keys, respectively,

- until said original message, propagated in the described snowball-like way, reaches its destination, i.e. said n-th lock or key.

12. A method for propagating information in an electronic lock-and-key system, characterized in that

- an original message to be propagated to an n-th lock or key is stored in a memory of a first lock,
- when a first key is used with said first lock, said original message is copied into said first key's memory but remains in said first lock's memory,
- when said first key is used with a second lock, said original message copied into said second lock's memory, but remains in said first key's memory,
- when a second key is used with said second lock, said original message is copied into said second key's memory, but remains in said second lock's memory,
- until said original message, propagated in the described way, reaches its destination, i.e. said n-th lock or key.

13. The method for propagating information according to claim 11, or claim 12, further characterized in that

- the n-th lock or key produces a confirmation message acknowledging reception of said original message which confirmation message serves to control erasing of the copies of the original message in the memories of the locks and keys.

14. The method for propagating information according to claim 13, further characterized in that

- the confirmation message is propagated through the system in the same way as the original message,

- said confirmation message, when received by a lock or key whose memory still contains a copy of said original message, acts on, in particular serves to erase said original message.

5   15. The method for propagating information according to any of the claims 11 to 14, further characterized in that

- after a selective or universal time-out, copies of said original message are selectively or universally erased.

10   16. The method for propagating information according to any of the claims 11 to 15, wherein

- original messages and/or confirmation messages, especially those concerning the same lock or key, are ordered, in particular sequentially numbered.

15   17.   The method for propagating information according to claim 16, further characterized in that

- any message of lower order, in particular with a lower sequence number, is erased in the respective memory when a message of higher order, in particular with a higher sequence number, is received by a lock or key during
20   propagation.

18. The method for propagating information according to any of the preceding method claims 11 to 17, wherein

- original messages and/or confirmation messages are fully or partly encrypted,
25   in particular using a shared key encryption scheme and/or a public key encryption scheme.